16TH ICCRTS

"Collective C2 in Multinational Civil-Military Operations"

Vulnerability of C2 Networks to Attack: Measuring the topology of eleven Dutch Army C2 systems

Topic:
Cyberspace Management

T.J. Grant, B.C. Buizer, R.J. Bertelink

Point of Contact:
Tim Grant

Netherlands Defence Academy
P.O. Box 90.002
4800 PA Breda
The Netherlands

Tel: +31 76 527 3261
Fax: +31 76 527 3259
tj.grant@nlda.nl

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2011		**00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Vulnerability of C2 Networks to Attack: Measuring the topology of eleven Dutch Army C2 systems	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Netherlands Defence Academy,P.O. Box 90.002,4800 PA Breda The Netherlands,**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
Presented at the 16th International Command and Control Research and Technology Symposium (ICCRTS 2011), Qu?c City, Qu?c, Canada, June 21-23, 2011. U.S. Government or Federal Rights License.

14. ABSTRACT
Effective C2 depends on a reliable networking infrastructure. Under current Royal Netherlands Army doctrine, C2 networks are designed to provide the connectivity, bandwidth, and low latency needed for military operations. Additionally, best practice provides redundancy against hardware and software failures. It is implicitly assumed that this redundancy also protects against the effects of enemy action. A recent development in mathematical network theory is the investigation of network resilience. Research shows that, depending on the topology, network robustness can differ greatly according to the way in which nodes or arcs are removed. In particular, scale-free networks are robust when nodes are removed randomly, but are vulnerable to targeted attack. To apply these results to the military domain, we need to measure the topology of existing C2 networks. In the 12th ICCRTS, Grant et al (2007) speculated that C2 networks, like the Internet and WWW, are scale-free networks. The purpose of this paper is to report the results of measuring the topology of eleven Royal Netherlands Army C2 systems, modelled as networks. These measurements confirm our speculation, with modelling guidelines emerging as a by-product of our research. We discuss the implications and make recommendations for doctrine and for further research.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**31**	

Vulnerability of C2 Networks to Attack: Measuring the topology of eleven Dutch Army C2 systems

Abstract

Effective C2 depends on a reliable networking infrastructure. Under current Royal Netherlands Army doctrine, C2 networks are designed to provide the connectivity, bandwidth, and low latency needed for military operations. Additionally, best practice provides redundancy against hardware and software failures. It is implicitly assumed that this redundancy also protects against the effects of enemy action.

A recent development in mathematical network theory is the investigation of network resilience. Research shows that, depending on the topology, network robustness can differ greatly according to the way in which nodes or arcs are removed. In particular, scale-free networks are robust when nodes are removed randomly, but are vulnerable to targeted attack. To apply these results to the military domain, we need to measure the topology of existing C2 networks.

In the 12th ICCRTS, Grant et al (2007) speculated that C2 networks, like the Internet and WWW, are scale-free networks. The purpose of this paper is to report the results of measuring the topology of eleven Royal Netherlands Army C2 systems, modelled as networks. These measurements confirm our speculation, with modelling guidelines emerging as a by-product of our research. We discuss the implications and make recommendations for doctrine and for further research.

Introduction

The literature on Network Enabled Capabilities (NEC) emphasizes the potential benefits of network-enabled operations. However, practical experience with similar socio-technical advances shows that, in real life, benefits are gained only at a cost. Nevertheless, it may still be worthwhile pursuing the benefits of such advances if the associated costs can be mitigated. To do so, the costs and ways of mitigating them must be understood. There is no reason to believe that NEC should be different from previous socio-technical advances.

In the 12th ICCRTS, Grant, van Fenema, van Veen, and Neerincx (2007) identified a potential danger lurking in the first two of the NEC tenets (Alberts, Garstka & Stein, 1999). These tenets claim that a robustly networked force improves information sharing and that information sharing enhances the quality of shared situation awareness. Grant et al asked themselves what would happen if the information being shared was erroneous. They enumerated the ways in which various sub-systems of a generic C2 system were fallible. When considering the underlying communications network, they identified the network's resilience to failure and its propensity to propagate errors as sources of fallibility.

The resilience of networks to failure and their error propagation properties are ongoing research areas in mathematical network theory (Newman, 2003). Researchers have shown that networks with the scale-free topology are resilient to random failure but vulnerable to targeted attack. Moreover, errors propagate readily in scale-free networks. Observing that the Internet and World Wide Web have been shown to be scale-free networks, Grant et al (2007) speculated that industrial-age C2 systems in hierarchical organizations are also likely to be scale-free. If so, then such C2 systems would be vulnerable to targeted attack, irrespective of whether this were kinetic or cyber.

We have now tested Grant et al's (2007) speculation. The purpose of this paper is to report on the results of measuring the topology of eleven Royal Netherlands Army C2 systems, modelled as networks. The second author completed this study as the capstone project (Buizer, 2010) to his three-year, bachelor-level Communications-, Information-, and Command & control Systems (CICS) course (Grant, 2009). The first and third authors supervised him, with the third author also providing subject matter expertise.

The paper consists of six sections. Section 1 is introductory. Section 2 outlines relevant aspects of the mathematical theory of network resilience. Section 3 describes the eleven C2 systems that were studied, as well as the doctrine followed in their design. Section 4 shows how these systems were modelled as networks, listing the modelling guidelines developed during the course of the study. Section 5 summarizes the results of measuring the topology of the subject networks. Section 6 draws conclusions and makes recommendations, both for further research and for changes to the current Royal Netherlands Army doctrine for designing C2 systems.

Some words on terminology are necessary here. We use "C2" as our portmanteau term, following the US DoD Joint Publication 1-02 definition of Command & Control. We do not distinguish between computers and communications, largely because the technologies are converging. In this paper, we use the term "C2 system" to mean the complete C2 system for the set of units taking part in a particular operation or exercise, encompassing all the DOTMLPFI[1] factors. In the NEC literature, a C2 system covers the physical, information, cognitive, and social domains. We use the term "C2 network" to mean that Materiel part of the C2 system that can be found in the physical domain, i.e. the computing and communications hardware and software. Note that this excludes the human users. To denote the mathematical representation of such a C2 network we have tried to use

[1] Doctrine, Organization, Training & education, Materiel, Leadership, Personnel, Facilities, and Interoperability.

the term “model” or “network” (without preceding “C2”). Discerning readers may observe that we have not always followed these conventions strictly. We trust that this will not lead to confusion.

Theory of Network Resilience

Networks, nodes, and arcs

Mathematical network theory has been successfully applied to social, information, technological, and biological networks (Newman, 2003). Networks (a.k.a. graphs) are modelled as collections of nodes (a.k.a. vertices) connected by arcs (a.k.a. edges). The number of nodes is generally denoted by *n*, and the number of arcs by *m*.

The communications network underlying a C2 system is an example of a technological network. Servers, hubs, routers, and end-user terminals can be modelled as nodes. The wired and wireless communication links connecting them can be modelled as arcs.

Network properties

A key property of a node is its degree, denoted *k*, i.e. the number of arcs that connect it to other nodes. The average node degree, $<k>$, is one common network property. Other common network properties are degree distributions, degree correlations, geodesic paths, the network diameter, clustering, various forms of centrality, and graph spectra (Boccaletti, Latora, Moreno, Chavez & Hwang, 2006).

For the purposes of measuring the topology of C2 systems, we need properties that are well understood in the literature, that discriminate the most common types of network, that are relevant to C2, and that are supported by readily available network analysis tools. Cares (2005, Appendix II, p.162-170) recommends a set of desirable properties for network-enabled C2. We chose the following properties:

- *Degree distribution*. Following Newman (2003), we define p_k to be the fraction of nodes in the network that have degree *k*. A plot of p_k for any given network can be formed by making a histogram of the degrees of nodes; this histogram is the network’s degree distribution, *P(k)*. In a random graph (Erdős & Rényi, 1959) the degree distribution is binomial or Poisson in the limit of large graph size.
- *Characteristic length*. The characteristic length *l* is the average geodesic path length of the network. A geodesic path is the shortest path between two nodes. There is no exact solution for *l* in the literature, but a number of partial exact results are known, as well as some approximate solutions for its behaviour as a function of the network’s parameters (Newman, 2003). In the limit where *p* tends to 0, the model is a “large world”. By contrast, small world behaviour is characterised by logarithmic scaling. For large *p* the model becomes like a random graph.
- *Cluster coefficient*. In many networks, it is found that if node A is connected to node B and node B to node C, then there is a heightened probability that node A is connected to node C. This is known as transitivity or clustering (Newman, 2003). In terms of network topology, clustering means the increased presence of triangles in the network. This can be quantified by defining a cluster coefficient, *C*, as three times the number of triangles in the network divided by the number of connected triples of nodes. In simple terms, *C* is the mean probability that two nodes that are network neighbours of the same other node will themselves be neighbours.

Types of network

Various types of network have been identified in the literature: random, small world, scale-free, regular, crystalline, and fully connected networks. The first three types have been investigated more extensively. Hence, our research focuses on random graphs (Erdős & Rényi, 1959), small worlds (Watts & Strogatz, 1998), and scale-free networks (Barabási & Albert, 1999).

The degree distribution, characteristic length, and cluster coefficient properties of random graphs, small worlds, and scale-free networks were obtained from the literature; see Table 1.

Table 1. Properties of random graphs, small worlds, and scale-free networks.

	Random	Small World	Scale-free
$P(k)$	$P(k) = \frac{e^{-\langle k \rangle}\langle k \rangle^k}{k!}$ (Bollobas, 1985)	$P(k) = \sum_{i=1}^{\min(k-\kappa,\kappa)} \binom{\kappa}{i}(1-p)^i p^{\kappa-i} \frac{(pk)^{k-\kappa-i}}{(k-\kappa-i)} e^{-pk}$ (Barrat & Weigt, 2008)	$P(k) \sim k^{-\gamma}$ (Barabási, 2002)
ℓ	$\ell \sim \frac{\ln n}{\ln\langle k \rangle}$ (Bollobas, 1985)	$p = 0: \ell \sim \frac{n}{2k} \gg 1$ $p \to 1: \ell \sim \frac{\ln n}{\ln\langle k \rangle}$ (Barrat & Weigt, 2008)	$\ell \sim \frac{\log n}{\log \log n}$ (Bollobas & Riordan, 2004)
C	$C = p$ (Watts & Strogatz, 1998)	$C(p) = \frac{3(\kappa-1)}{2(2\kappa-1)}(1-p)^3$ (Barrat & Weigt, 2008)	$C(k) \sim k^{-0,75}$ (Albert & Barabási, 2002)

Network resilience

Many complex systems display a surprising degree of tolerance to errors, attributed to the robustness of the underlying network. In network theory, robustness is modelled by the removal of nodes or arcs (Newman, 2003). Albert, Jeong, and Barabasi (2000) demonstrate that error tolerance is not shared by all redundant systems, but is displayed only by scale-free networks. However, error tolerance comes at a price, because these networks are extremely vulnerable to targeted attacks, i.e. to the selection and removal of the nodes that play the most important role in assuring the network's connectivity.

Figure 1 summarises Albert et al's (2000) results. The upper half of the figure shows the response to random failures and the lower half shows the response to targeted attacks. Exponential networks (including random graphs and small worlds) under both random failures and targeted attack behave similarly to scale-free networks under attack. For small error rates, *f*, there is still a large cluster (Figure 1a). At a critical f_c (Figure 1b), the network breaks into small fragments. The network fragments further as the error rate increases (Figure 1c). By contrast, scale-free networks show a different scenario under random failure. The size of the largest cluster decreases slowly. The large cluster persists, even at unrealistically high error rates (Figure 1f).

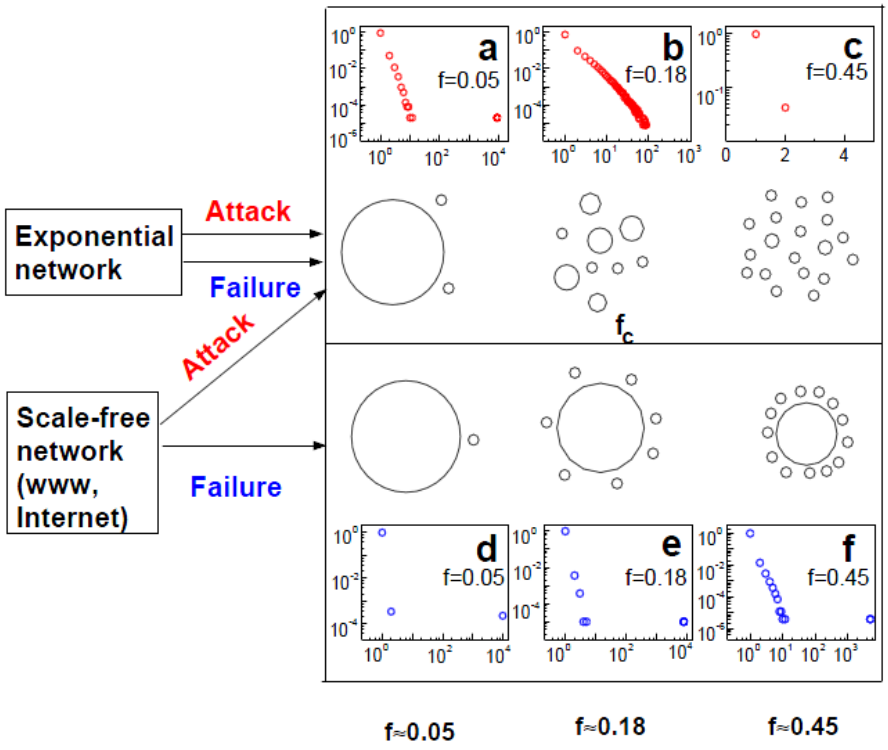


Figure 1. Summary of network response to failures or attacks (Albert, Jeong & Barabási, 2000, Fig 4).

C2 Systems Studied

Designing C2 systems is not an exact science. Study of Royal Netherlands Army manuals and interviews of C2 system architects disclosed that there are several steps in designing a C2 system for a particular mission:

- At a higher level, decisions are made on which units will take part in the mission and which C2 applications they will use.
- Knowing which units will take part and what C2 applications they will use, the architect:
  - determines the connectivity between these units and what bandwidth they need.
  - selects a set of building blocks that will provide this connectivity and bandwidth.
  - chooses the appropriate terrestrial wireless or satellite communications links, based on the likely distance separating the units and the terrain in which they are placed.
  - adds redundancy to cope with likely failures, based on his/her experience.

Under current doctrine, the architects do not consider the vulnerability of the C2 system to attack, nor do they apply measures drawn from network theory in assessing the adequacy of the design. When asked, they say that they assume that redundancy to cope with failure also protects against the effects of enemy action.

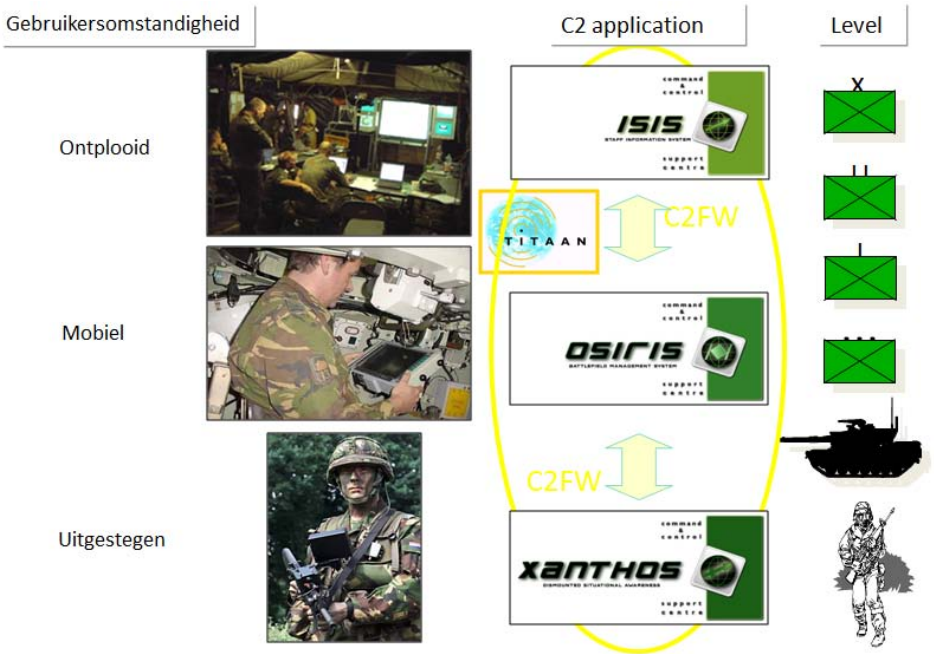


Figure 2. The Royal Netherlands Army's family of C2 systems.

The Royal Netherlands Army has three families of C2 systems (see Figure 2): the Integrated Staff Information System (ISIS) for static and deployed ("ontplooid") applications, the Battlefield Management System (BMS, a.k.a. Osiris) for vehicle-mounted ("mobiel") applications, and the Soldier Digital Assistant (SDA, a.k.a. Xanthos) for dismounted ("uitgestegen") soldiers. The communications infrastructure underlying ISIS is IP-based, and is named the Theatre Independent Tactical Army & Air force Network (TITAAN). Combat net radio provides the communications infrastructure underlying BMS/Osiris and SDA/Xanthos.

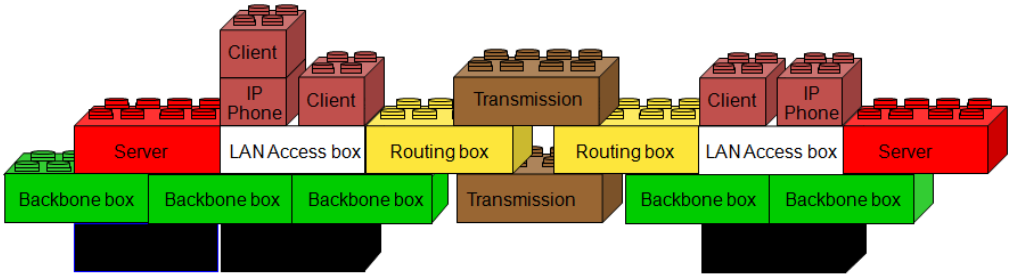


Figure 3. TITAAN building blocks.

TITAAN is a collection of components that can be assembled like building blocks; see Figure 3. The base component is the local area network (LAN) access box. Office equipment, such as user terminals, printers, plotters, scanners, and servers are brought under this component. LAN access boxes can be connected into a wide-area network (WAN) using routing and backbone boxes. Client applications include ISIS, voice-over-IP (VoIP) telephony, military email, and chat. Figure 4 shows selected components. The upper row from left to right shows a radio vehicle, a user terminal, and a VoIP telephone. The lower row shows a tactical satellite terminal and a command post with a double radio link.

Figure 4. TITAAN components.

BMS is the ruggedized C2 system for vehicle mounting, providing blue-force tracking functionality based on the vehicle's GPS location. BMS units in different vehicles exchange information peer-to-peer. Osiris is the C2 client application that runs in the BMS environment. The Advanced Fire Support Information System (AFSIS) is a variant of Osiris for the fire support chain; see Figure 5.

Figure 5. AFSIS terminals in a PxH2000 howitzer.

Modelling C2 Systems in Network Theory Terms

We gathered the designs of eleven C2 systems, covering deployed and mobile land operations. Three were TITAAN networks, two BMS, two Osiris, and four AFSIS. All but one of the networks were designed for exercise purposes, with the remaining network being used for operationally-realistic testing of TITAAN. Figure 6 shows an example network.

Figure 6. Example AFSIS network.

The first step in measuring the topology of each network was to model it in network theory terms. This required us to identify nodes and arcs. In doing so, we encountered a number of modelling issues that we had to address in a uniform way across all eleven networks. The issues and the guidelines that we adopted for modelling them uniformly were as follows:

- *Entity types*. The networks included different types of real-world entities. All included routers and hubs, but some omitted the end-user terminals. As Figure 6 shows, many networks included both wired and wireless links. Moreover, these links had different capacities and classifications. For modelling purposes, we made no distinction between entity types or between link types. Each entity was modelled as a node regardless of its type, and similarly each link regardless of type was modelled as an arc. Nodes and arcs were non-valued, i.e. we ignored differences in capacity and classification.
- *System boundary*. Most networks included interfaces to one or more other networks. For example, a BMS network in the mobile domain might have an interface to TITAAN in the deployed domain. In this case, we modelled each other network as a single node, because the other network is outside the boundary of the system we were studying.
- *End-user terminals*. We modelled the end-user terminals as nodes. Where end-user terminals were not shown in the C2 network, we assumed that an average LAN access box (LAB) would have six end-user terminals. The inclusion of end-user terminals has consequences

for the vulnerability of the network to attack that are dependent on the type of attack. Given the short distance between LABs and their attached end-user terminals, a targeted attack on a LAB would also bring down the attached end-user terminals. By contrast, a random failure would be likely to affect only the component that suffered the failure.

- *Wireless "clouds"*. Six of the mobile networks include wireless "clouds". This implies that all the entities linked to a cloud can also communicate directly to each other, assuming that a broadcast technology (such as radio) is used, that all entities are on the same frequency, and that no terrain intervenes between any sub-group of entities. In effect, a "cloud" could then be modelled as a fully-connected sub-network. This would accurately model the behaviour of the "cloud" in the face of a random attack, but not a targeted attack on the "cloud", such as jamming. To model both types of attack adequately, we chose to model a "cloud" as a central node to represent the "ether" to which all the entities using the "cloud" are linked. Jamming could then be represented by removal of the "ether" node.

Using the guidelines we adopted, the example AFSIS network shown in Figure 6 was modelled as shown in Figure 7.

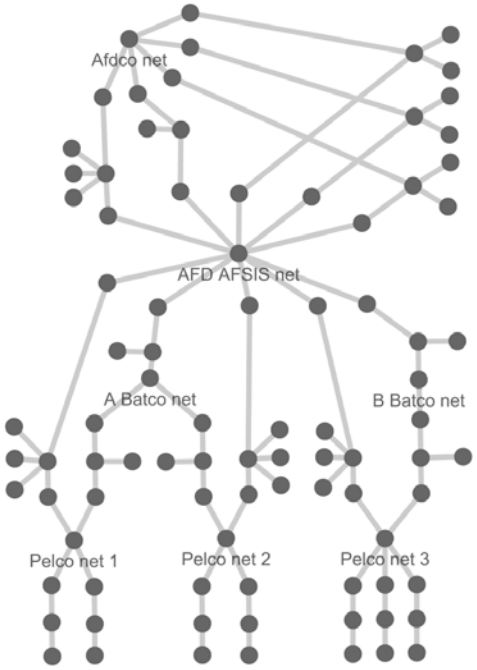


Figure 7. Model of the example AFSIS network.

Simple properties (i.e. operational environment, number of nodes, number of arcs, and average degree) for the eleven C2 systems we modelled are shown in Table 2.

Network name	Environment	n	m	$\langle k \rangle$
FAT 018 strz	Deployed	171	191	2.222
TITAAN v021	Deployed	88	103	2.25
TITAAN41 SYST	Deployed	141	153	2.17
AFSIS 3.2 afd	Mobile	90	96	2.133
AFSIS 3.2 afd man	Mobile	84	88	2.095
AFSIS 3.2 bt	Mobile	76	80	2.105
AFSIS 3.2 man mr	Mobile	79	81	2.051
OSIRIS 3.0 A	Mobile	44	43	1.955
OSIRIS 3.0 B	Mobile	56	58	2.071

BMS 3.1 A	Mobile	94	106	2.191
BMS 3.1 B	Mobile	55	64	2.327

Table 2. Simple properties for the eleven C2 systems (Buizer, 2010, Table 3.1, p.28).

In reaching the guidelines adopted (as described above), we tested a variety of possible alternatives. We found that the resulting measurements for the eleven networks were sensitive to the guidelines chosen. Therefore, we regard our development of modelling guidelines as an important secondary contribution of this paper. Nevertheless, other researchers should scrutinize the modelling guidelines closely when applying them to networks different in nature to our eleven.

Results of Topology Measurements

The topology measurements were obtained using the Cytoscape software tool[2], together with its NetworkAnalyser plug-in[3].

The detailed numerical results (power, characteristic path length, and cluster coefficient) for the eleven modelled C2 systems ("real") and their equivalent random graphs ("rand") are shown in Table 3.

Network name	γ	ℓ_{real}	ℓ_{rand}	C_{real}	C_{rand}
FAT 018 strz	1.996	9.723	6.440	0.034	0.013
TITAAN v021	1.804	6.763	5.212	0.073	0.026
TITAAN41 SYST	1.521	9.85	6.388	0.053	0.015
AFSIS 3.2 afd	1.573	6.412	5.925	0	0.024
AFSIS 3.2 afd man	1.734	10.489	5.991	0	0.025
AFSIS 3.2 bt	1.749	5.913	5.818	0	0.028
AFSIS 3.2 man mr	2.049	8.439	6.083	0	0.026
OSIRIS 3.0 A	1.775	7.44	5.645	0	0.044
OSIRIS 3.0 B	1.595	7.623	5.529	0	0.037
BMS 3.1 A	1.459	8.443	5.792	0.073	0.023
BMS 3.1 B	1.645	7.294	4.745	0.135	0.042

Table 3. Numerical results for eleven C2 systems (Buizer, 2010, p.63).

[2] http://www.cytoscape.org/.
[3] http://med.bioinf.mpi-inf.de/netanalyzer/.

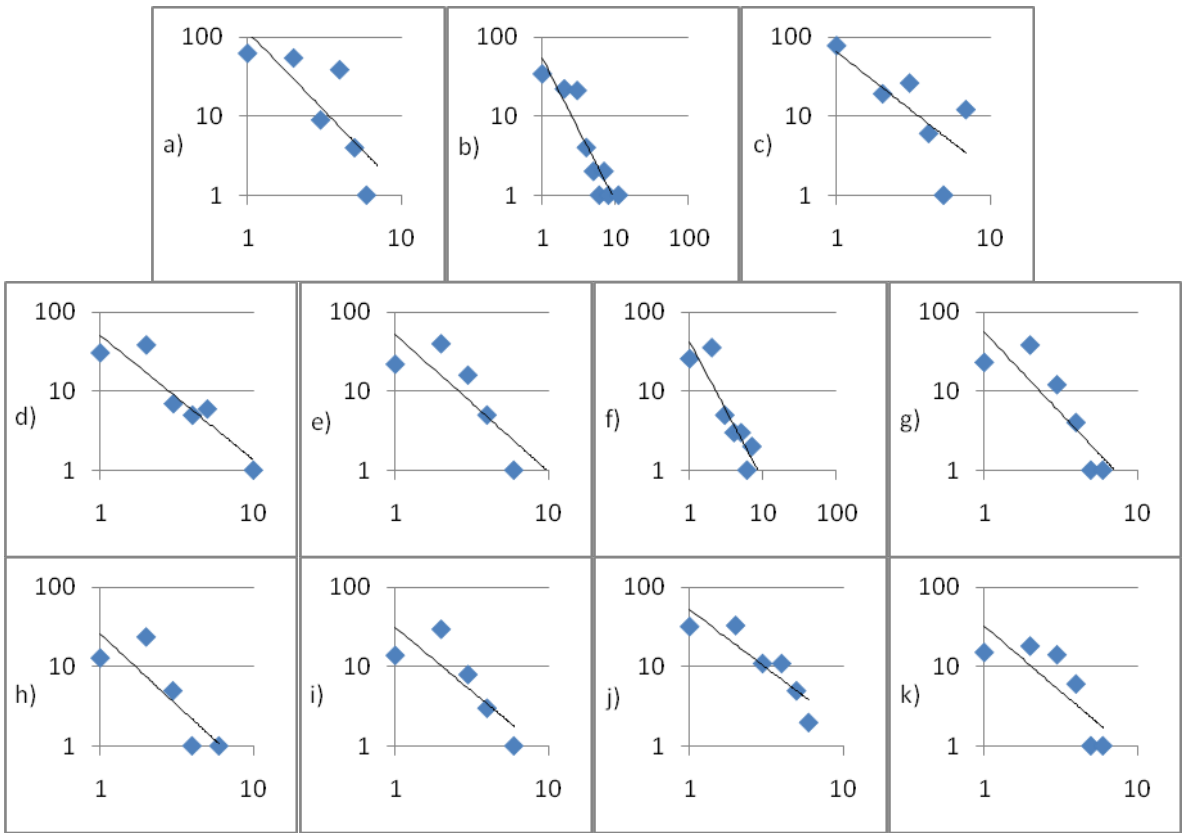


Figure 8. Results for degree distribution (log-log plots) (Buizer, 2010, Figure 5.1, p.33).

All networks show an approximate power-law form when plotted on log-log coordinates; see Figure 8. The form is approximate because each network is upper-truncated, with a low frequency for nodes with a degree of 1. This is typical of small networks, i.e. around 100 nodes or less (Cares, 2005). Cytoscape obtained the powers shown in Table 3 by finding the best fit to a power law for each histogram.

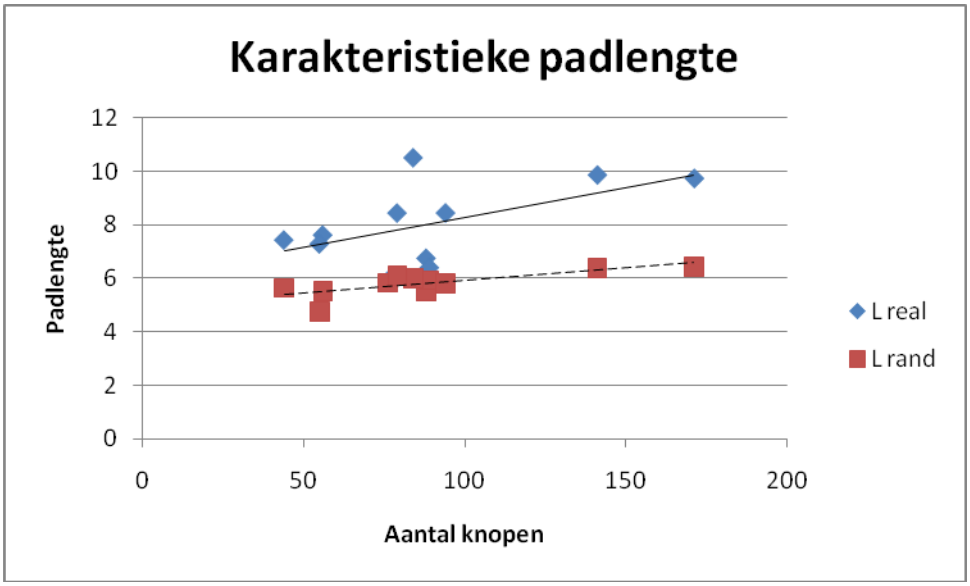


Figure 9. Results for characteristic path length (Buizer, 2010, Figure 5.2, p.34).

To determine whether the characteristic path length is short or long, we compared the measurements to equivalent random graphs. As Figure 9 shows, the normalised path length for the eleven modelled networks ("L real", blue diamonds) is clearly longer than the characteristic path

length for a random graph with the same number of nodes and average degree (“L rand”, red squares).

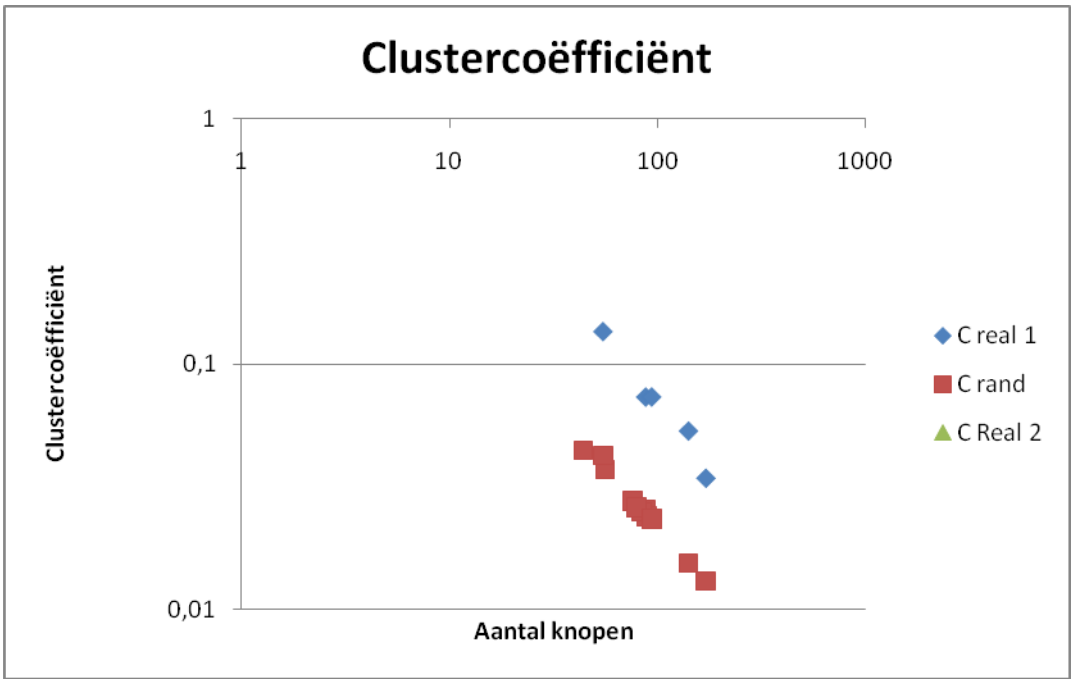


Figure 10. Results for cluster coefficient (Buizer, 2010, Figure 5.4, p.36).

As for characteristic path length, the cluster coefficients for the modelled networks were compared with the equivalent random graphs; see Figure 10. The cluster coefficient for six of the networks (“C real 2”, not shown in Figure 10) was ten times the cluster coefficient of the other five (and of their equivalent random graphs). These six networks – all four AFSIS networks and all two Osiris networks - contained wireless “clouds”. We believe that this behaviour is an artefact of our modelling guidelines. For the remaining five networks without “clouds” (“C real 1”, blue diamonds), the cluster coefficient is higher than that for the equivalent random graph (“C rand”, red squares).

Summarising these results, we see that our eleven C2 networks exhibit a truncated power-law form and have a higher characteristic path and a higher cluster coefficient than the equivalent random graphs. Regarding the three properties as dimensions, we depict the results qualitatively in Figure 11. The scales should not be seen as being metric. The networks we studied (“Onderzochte netwerken”) are closer to the theoretical scale-free (“Schaalvrij”) properties, than to the theoretical properties for random graphs (“Willekeurig”) or for small worlds.

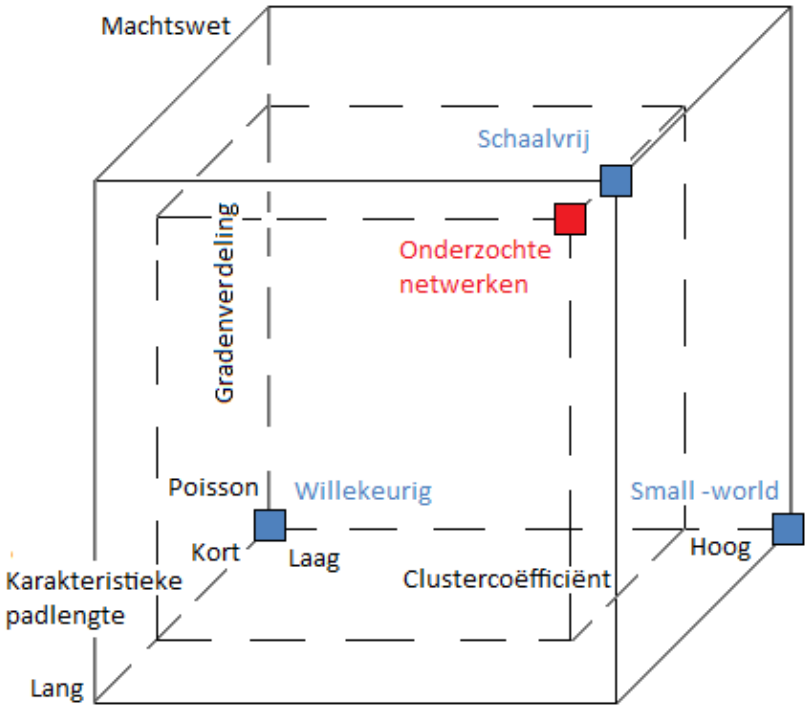


Figure 11. Depicting the results qualitatively in three dimensions (Buizer, 2010, Figure 5.5, p.37).

Conclusions and Recommendations

This paper reports on the results of measuring the topology of eleven Royal Netherlands Army C2 systems, modelled as networks. In previous work (Grant et al, 2007), we had speculated that C2 systems were likely to be scale-free networks. The paper outlines the relevant aspects of the mathematical theory of networks, describes the eleven C2 systems we studied, shows how they were modelled, and summarises the results. We conclude that the C2 systems we studied were indeed closest in form to scale-free networks, like the Internet and the World Wide Web. More details of our study can be found in Buizer (2000).

Our research has many limitations. The most important are as follows:

- The number of C2 systems modelled is too small for statistical confirmation. Therefore, our conclusion that they exhibit scale-free behaviour can only be regarded as a qualitative indication[4].
- Only two of the eleven networks were more than 100 nodes in size. Cares (2005) states that networks should be at least 100 nodes for there to be significant network effects.
- All the networks were from the Royal Netherlands Army, i.e. the study is single-nation and single-service. Army C2 systems from larger nations are likely to be larger in size.
- All the C2 systems studied (bar one) were designed for exercises. They may not necessarily be representative of operational C2 systems. However, the “train as you fight, fight as you train” principle suggests that they should be close to the behaviour of operational C2 systems.
- Assessment shows that the Netherlands armed forces are between NEC Maturity Level 2 and 3. It may be that C2 systems from other nations or from coalitions with a higher NEC Maturity Level differ in behaviour.

[4] Readers might like to consider that similar results for the Internet and for the World Wide Web are in each case based on a sample of one.

Despite these limitations, we believe that this piece of research offers a significant research contribution. Firstly, it confirms Grant et al's (2007) speculation. Secondly, it adds to the scientific body of knowledge about real-life networks, because measurements of the topology of C2 networks do not appear to be in the open scientific literature. Thirdly, if our results are confirmed by other researchers, this has implications for C2 systems design in that existing practices – at least in the Royal Netherlands Army – result in systems that are vulnerable to targeted attack (whether this be kinetic or cyber in nature). A secondary contribution is that this paper reports on the modelling guidelines we adopted, enabling replication of results for other C2 systems and critical review of the guidelines for C2 systems from other nations and services.

Based on these results, we make the following recommendations:

- Further research is needed. In particular, our methods should be replicated for other services' and for other nations' C2 systems to see if similar results are obtained. Investigation should be extended to multinational civil-military operations and coalition C2 systems. The modelling guidelines need further study because they still result in modelling artefacts, especially with regards to the modelling of wireless communication networks.
- Doctrine for designing C2 systems needs to take account of network topology and its implication for vulnerability to failure and attack.

We speculate further that the apparently scale-free form of existing C2 networks may reflect the hierarchical command structure that they support. Even if hierarchical command structures cannot be eliminated (as NEC theory calls for), it may still be possible to disguise the topology of C2 systems, by structuring them in a form that is more resilient to targeted attack, such as a small world. This speculation needs more detailed study.

References

Albert, R., & Barabási, A-L. 2002. Statistical mechanics of complex networks. *Review of Modern Physics, 74*, 47-97

Albert, R., Jeong, H., & Barabási, A-L. 2000. Error and attack tolerance of complex networks. *Nature, 306*, 378-382

Alberts, Garstka & Stein. 1999. Network Centric Warfare. US DoD Command & Control Research Program, Washington D.C.

Barabási, A-L. *Linked.* New York: Perseus Publishing, 2002

Barabási, A-L, & Albert, R. Emergence of Scaling in Random Networks. *Science*, 1999: 509-512

Barrat, A., & Weigt, M. On the properties of small-world network models. *European Physics Journal B, vol. 13*, 2008: 547-560

Boccaletti, S., Latora, V., Moreno, Y., Chavez, M., & Hwang, D-U. 2006. Complex networks: Structure and dynamics. *Physics Reports, 424*, 175 – 308

Bollobás, B. 1985. *Random Graphs.* London: Academic Press

Bollobás, B., & Riordan, O. 2004. The diameter of a scalefree random graph. *Combinatorica, 14, 1*, 5-34

Buizer, B.C. 2010. Netwerkstructuren van C2-netwerken. Unpublished bachelor dissertation, Netherlands Defence Academy, Breda, Netherlands. [Title in English: Structure of C2 networks.]

Cares, J. 2005. *Distributed Networked Operations: The Foundations of Network Centric Warfare.* Newport, Rhode Island: Alidade Press

Erdős, P., & Rényi, A. 1959. On Random Graphs. I. *Publicationes Mathematicae Debrecen, 6*, 290–297

Grant, T.J. 2009. CICS – A Bachelor Degree for NEC-era Signals, ICT, and C2 Officers. In Alberts, D.S. (ed.), *Proceedings, 14th International Command & Control Research & Technology Symposium (ICCRTS09)*, US DoD Command & Control Research Program, Washington DC, paper

I-067
Grant, T.J., van Fenema, P., van Veen, M., & Neerincx, M. 2007. On Regarding 21st Century C2 Systems and their Users as Fallible ePartners. In Alberts, D.S. (ed.), *Proceedings, 12th International Command & Control Research & Technology Symposium (ICCRTS07)* , US DoD Command & Control Research Program, Washington DC, paper I-157.
Newman, M.E.J. 2003. The structure and function of complex networks. *SIAM Review,* 45, 2, 167-256.
Watts, D.J., & Strogatz, S.H. 1998. Collective dynamics of 'small-world' networks. *Nature, 393*, 440-442

Ministry of Defence

Vulnerability of C2 Networks to Attack: Topology of 11 Dutch Army C2 systems

Tim Grant *, Barend Buizer, & Ron Bertelink

* Netherlands Defence Academy (NLDA)
TJ.Grant@NLDA.nl
Tel: +31 76 527 3261 Mob: +31 638 193 749

Outline

Goal:

- To report the results of measuring the topology of 11 Royal Dutch Army C2 systems, modelled as networks

Overview:

- Motivation
- C2 systems studied
- Modelling C2 systems as networks
- Results of topology measurements
- Conclusions & recommendations

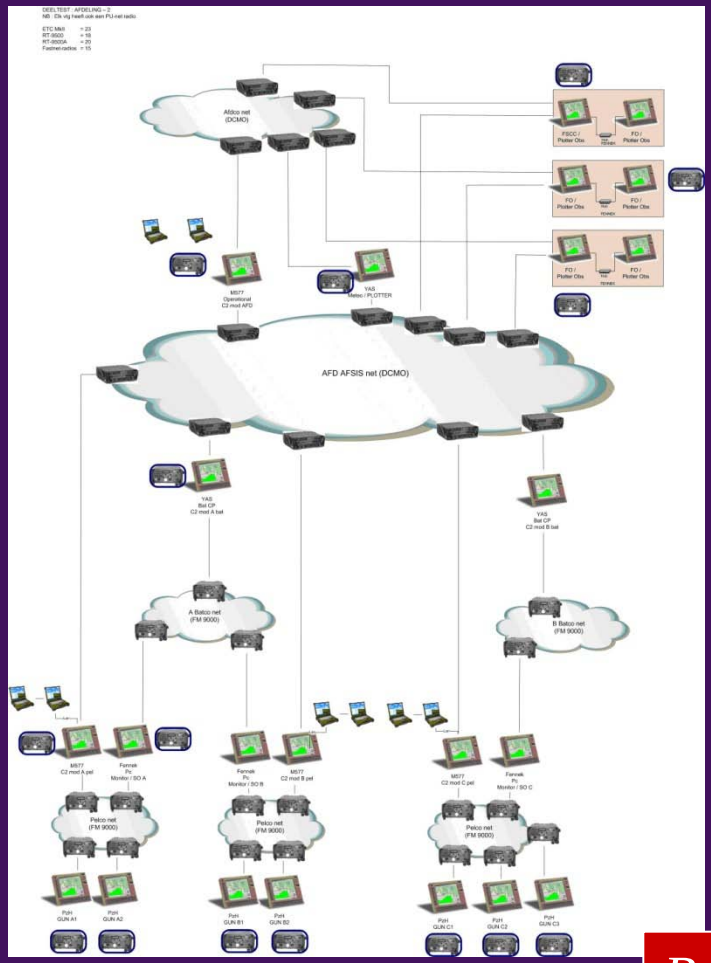
Motivation (1)

Mathematical network theory:

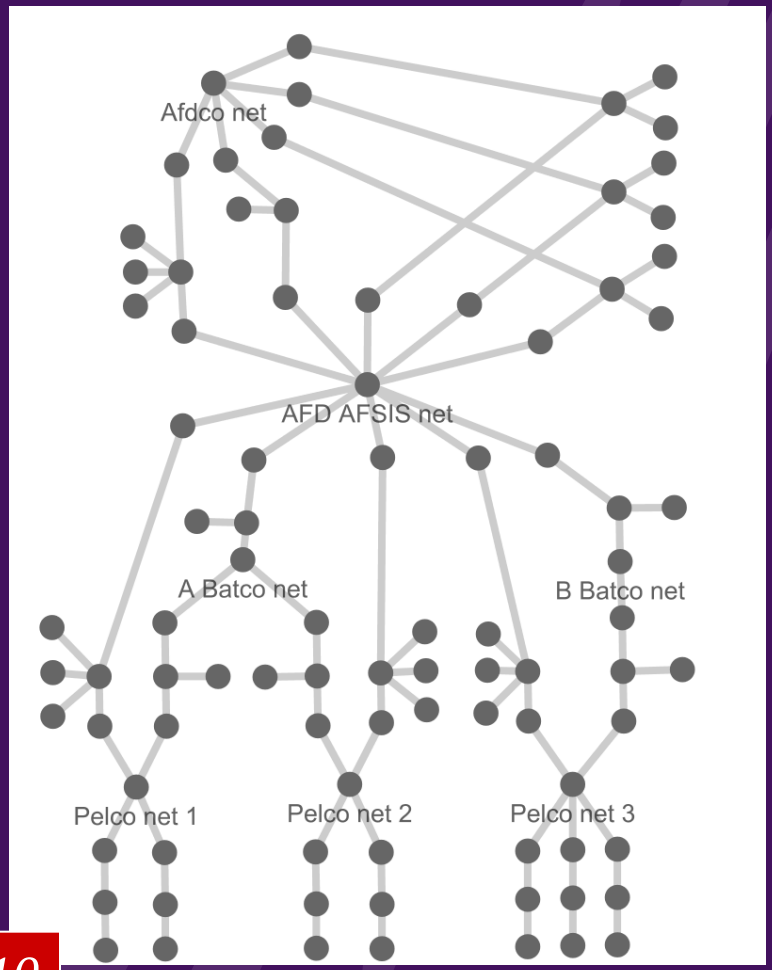
- Biological, social, knowledge, & technical applications
- Network = set of nodes & set of arcs
  - C2 system can be modelled as:
    - Nodes = users, workstations, routers, hubs
    - Arcs = (tele)communications links
- Major theoretical results since 2000:
  - Attacks modelled as removal of nodes
  - Attacks can be random or targeted
  - Types = random graphs, small worlds, scale-free
  - How these 3 types break up after attack

Motivation (2)

(Technical) system

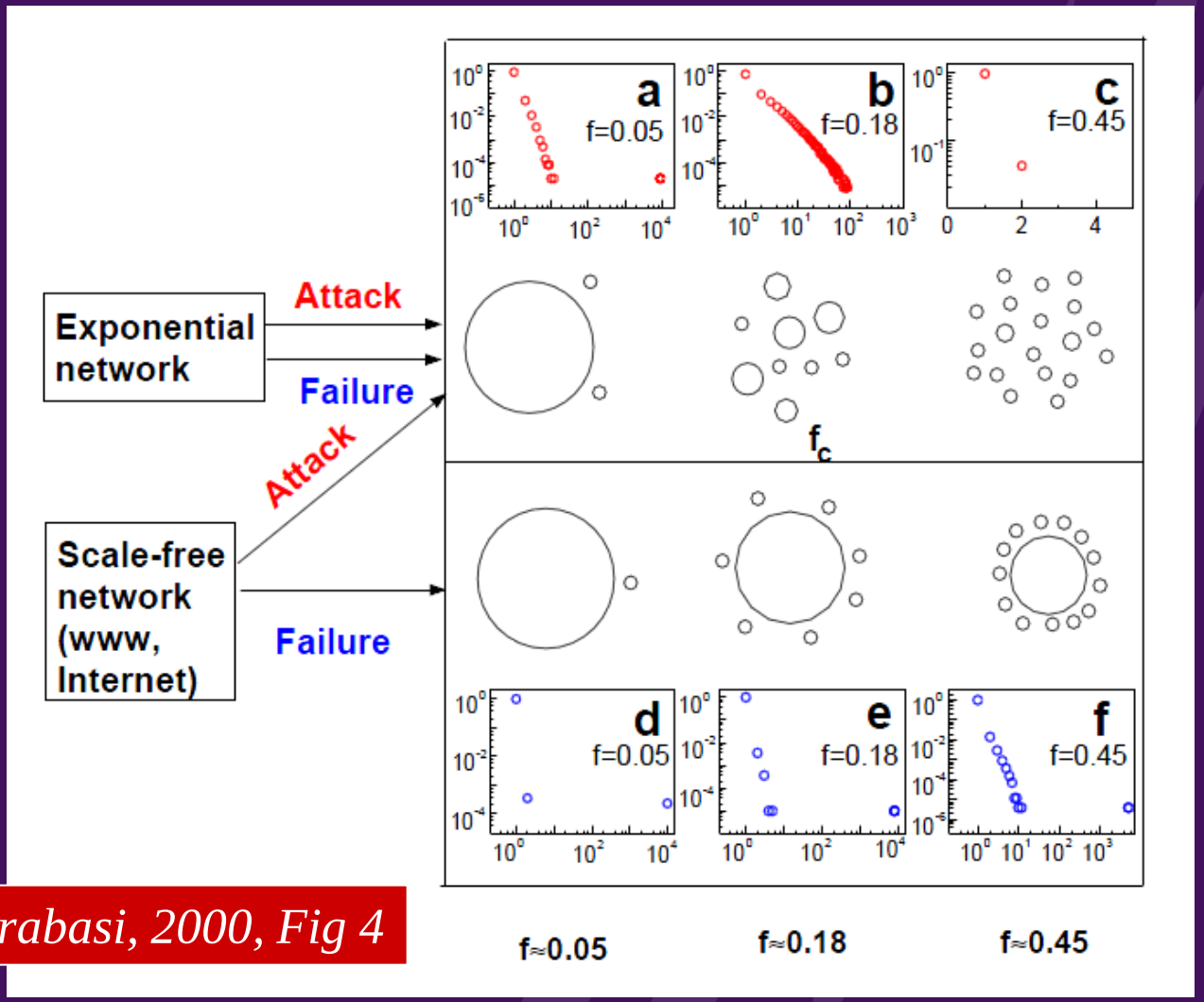


Network model of system



Buizer, 2010

Motivation (3)



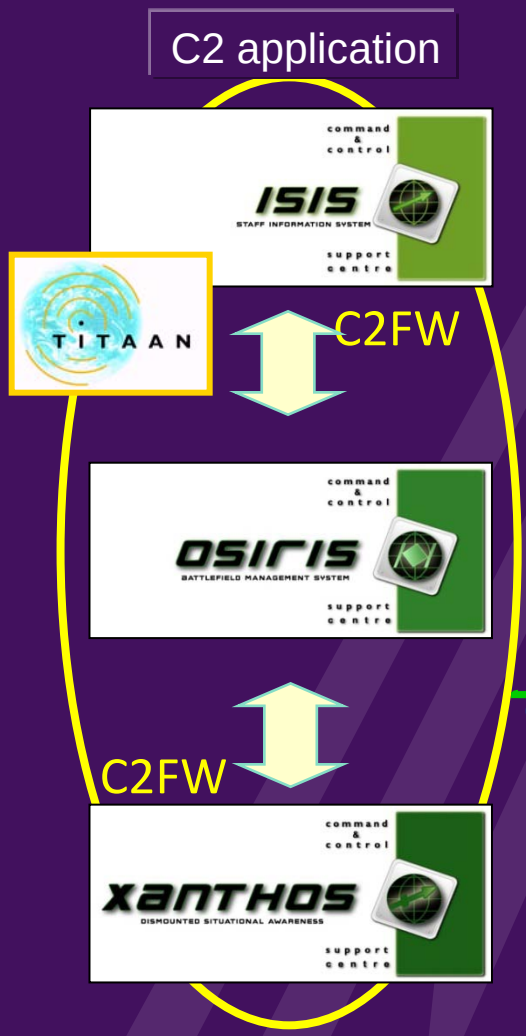
Alberts, Jeong & Barabasi, 2000, Fig 4

C2 systems studied (1)

Deployed

Mobile

Dismounted



C2 systems studied (2)

Network name	Environment	*n*	*m*	<*k*>
FAT 018 strz	Deployed	171	191	2.222
TITAAN v021	Deployed	88	103	2.25
TITAAN41 SYST	Deployed	141	153	2.17
AFSIS 3.2 afd	Mobile	90	96	2.133
AFSIS 3.2 afd man	Mobile	84	88	2.095
AFSIS 3.2 bt	Mobile	76	80	2.105
AFSIS 3.2 man mr	Mobile	79	81	2.051
OSIRIS 3.0 A	Mobile	44	43	1.955
OSIRIS 3.0 B	Mobile	56	58	2.071
BMS 3.1 A	Mobile	94	106	2.191
BMS 3.1 B	Mobile	55	64	2.327

Buizer, 2010, Table 3.1, p.28

Modelling C2 systems as networks

Guidelines adopted for uniform modelling:

- Entity types:
  - Could be routers, hubs, end-user terminals, etc
  - All modelled as nodes, regardless of type
  - Nodes & arcs non-valued
- System boundary:
  - System could have interface(s) to other network(s)
  - Each other network modelled as single node
- End-user terminals:
  - When end-user terminals not shown, 6 assumed
- Wireless “clouds”:
  - Central node to model (jammable) “ether”

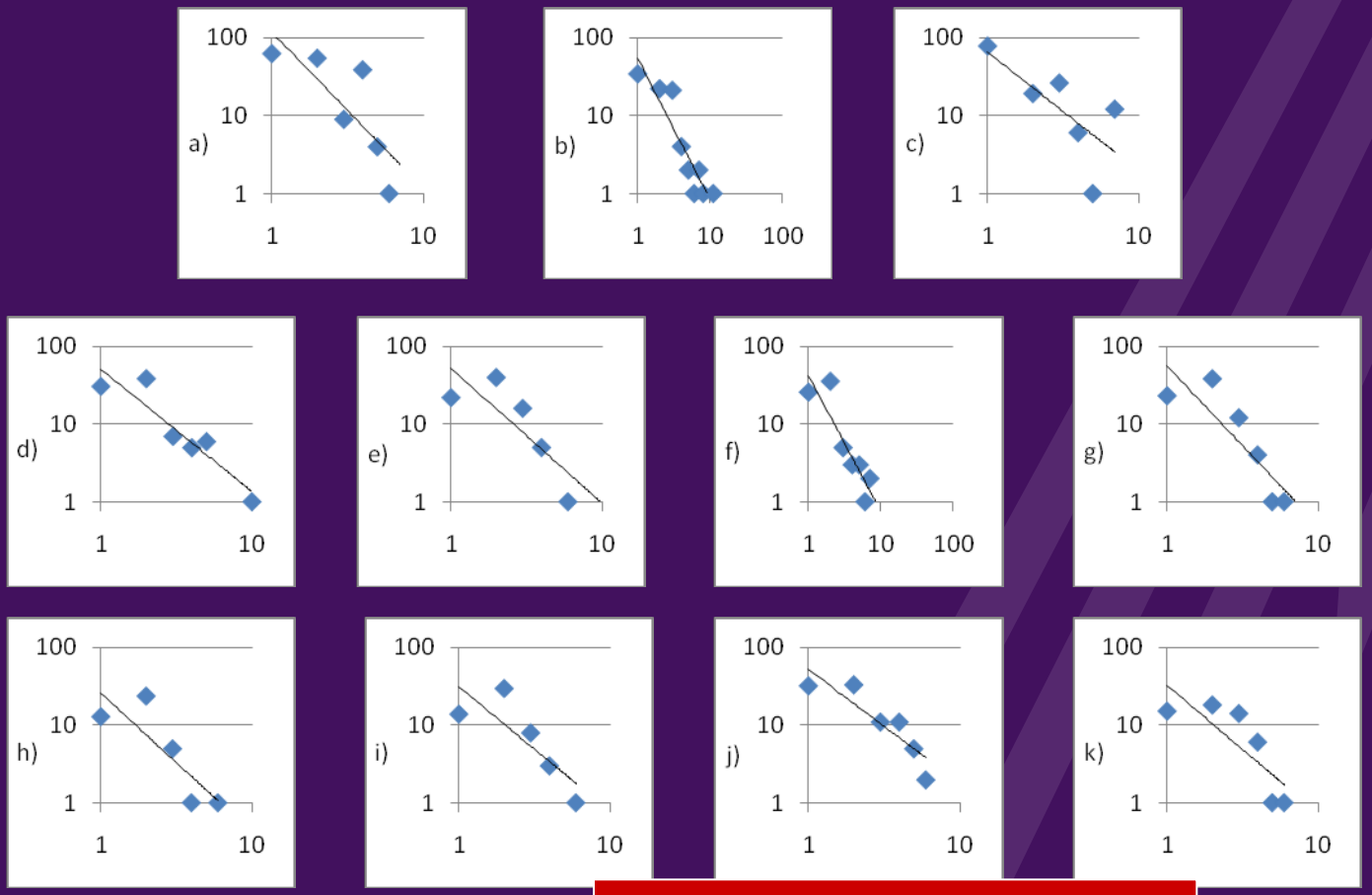
Results of topology measurements (1)

Network name	Power	Real length	Rand length	Real coeff	Rand coeff
FAT 018 strz	1.996	9.723	6.440	0.034	0.013
TITAAN v021	1.804	6.763	5.212	0.073	0.026
TITAAN41 SYST	1.521	9.85	6.388	0.053	0.015
AFSIS 3.2 afd	1.573	6.412	5.925	0	0.024
AFSIS 3.2 afd man	1.734	10.489	5.991	0	0.025
AFSIS 3.2 bt	1.749	5.913	5.818	0	0.028
AFSIS 3.2 man mr	2.049	8.439	6.083	0	0.026
OSIRIS 3.0 A	1.775	7.44	5.645	0	0.044
OSIRIS 3.0 B	1.595	7.623	5.529	0	0.037
BMS 3.1 A	1.459	8.443	5.792	0.073	0.023
BMS 3.1 B	1.645	7.294	4.745	0.135	0.042

Buizer, 2010, p.63

Results of topology measurements (2)

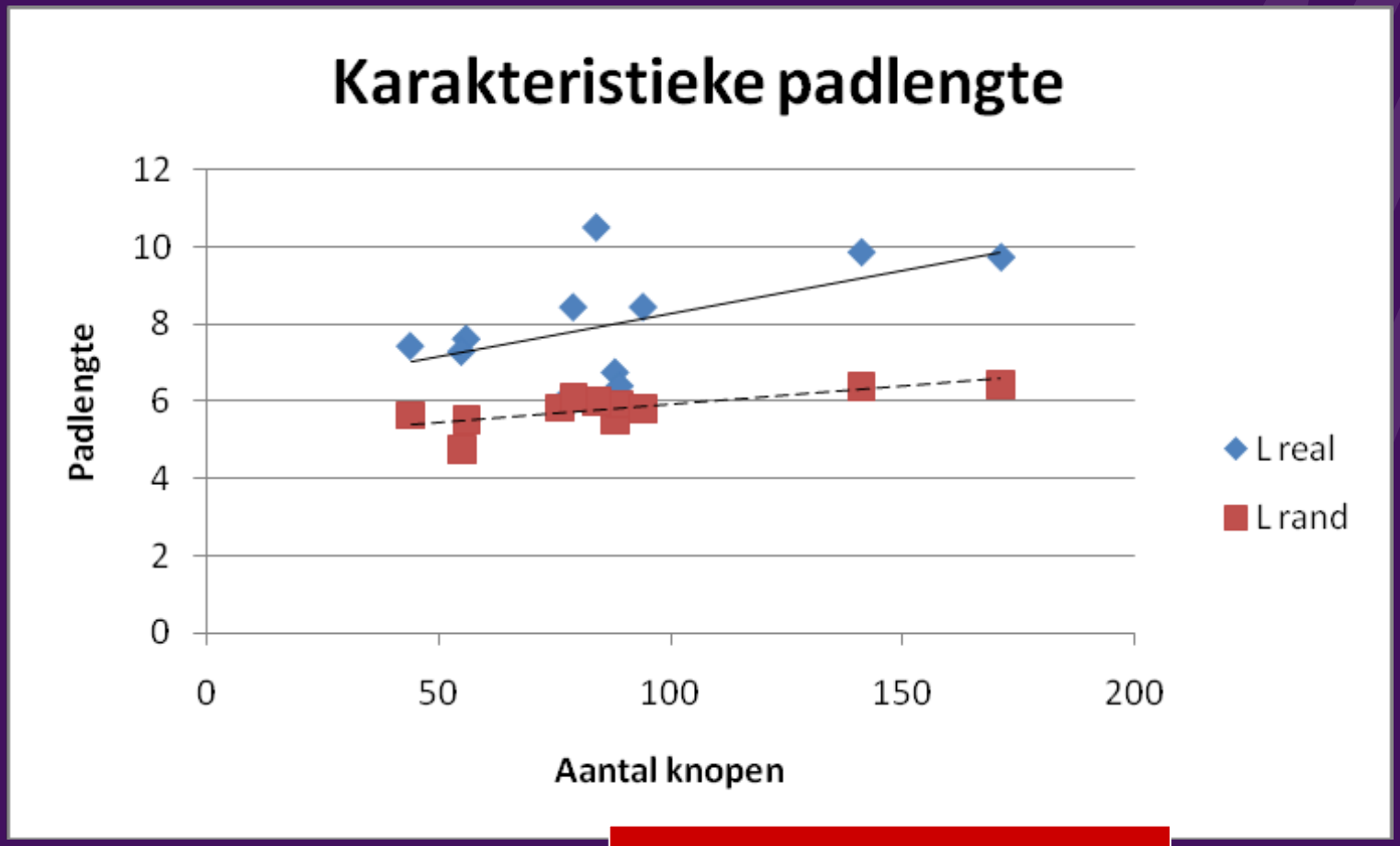
Degree distribution (log-log plots):



Buizer, 2010, Fig 5.1, p.33

Results of topology measurements (3)

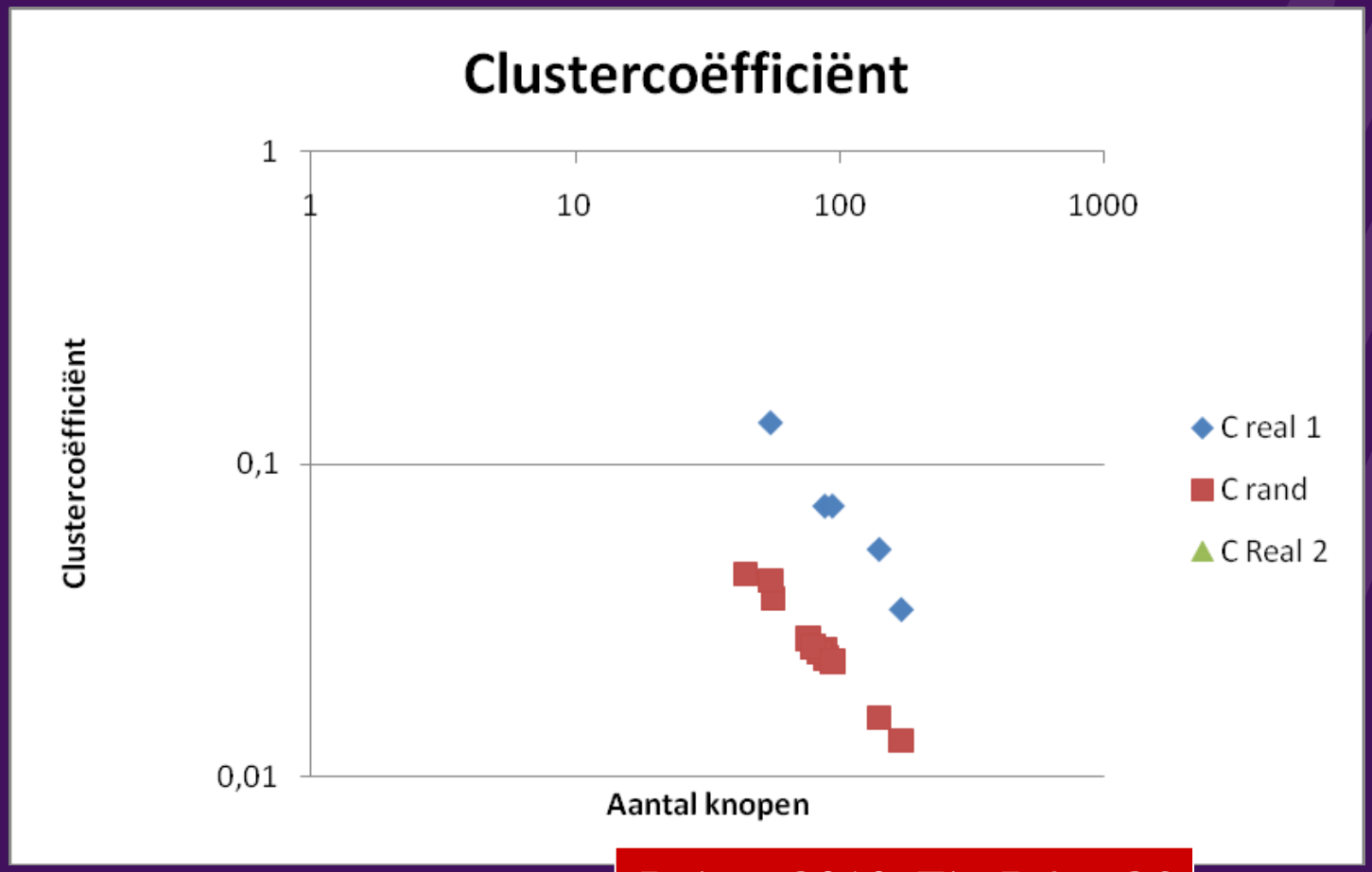
Characteristic path length:



Buizer, 2010, Fig 5.2, p.34

Results of topology measurements (4)

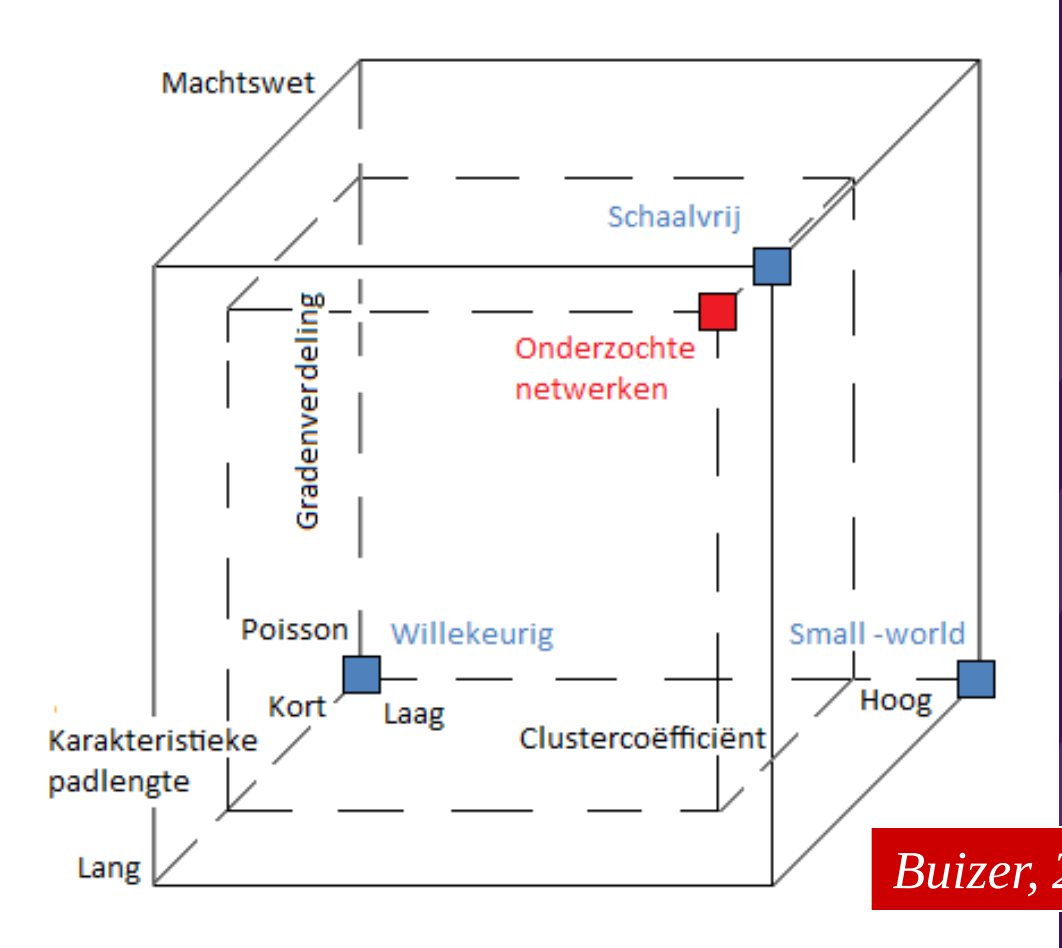
Cluster coefficient:



Buizer, 2010, Fig 5.4, p.36

Results of topology measurements (5)

Researched networks closest to scale-free:



Buizer, 2010, Fig 5.5, p.37

Conclusions & recommendations

Conclusion:

- C2 systems we studied closest to scale-free:
  - Like Internet and WWW
  - Confirms speculation in Grant et al, 2007 (12th ICCRTS)
- May reflect hierarchical command structure

Consequence:

- C2 systems likely to be vulnerable to targeted attack

Recommendations:

- Study other services' & nations' C2 systems
- Doctrine for C2 system design should consider network topology & its implication for vulnerability

Any questions?